

REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 1-44 are pending in this application.

35 U.S.C. § 102

Claims 1-29 and 32-44 stand rejected under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 6,577,734 to Etzel et al. (hereinafter "Etzel"). Applicant respectfully submits that claims 1-29 and 32-44 are not anticipated by Etzel.

Etzel is directed to a data encryption key management system (see, Title). In Etzel, when an instruction to encrypt a video program is received, a security module 30 uses an encryption key to encrypt a digital video stream and store the encrypted video signals in a server (see, col. 3, lines 49-58, and col. 4, lines 14-19). Once the program is encrypted and stored, the module 30 sends an encrypted version of the program encryption key to Access Control System (ACS) 40 (see, col. 4, lines 20-25). ACS 40 can then distribute that key in a similar secure manner to a user who has entered a request to review the program (see, col. 4, lines 25-30). Etzel also discusses a CV key, which is a shared symmetrical encryption key that is shared between two security modules (see, col. 5, lines 35-41). This CV key is used to encrypt the program encryption key so that the encrypted program encryption key can be sent to another security module (see, col. 5, lines 57-66).

In contrast, claim 1 recites:

One or more computer-readable media having stored thereon a plurality of instructions that, when executed by one or more processors of a computer, causes the one or more processors to perform the following acts:

receive a request, corresponding to a user, to access a file;
obtain an access control entry that corresponds to both the user and the file, wherein the access control entry includes an encrypted symmetric key that was used to encrypt the file;

check whether a mapping of the access control entry to the symmetric key exists in an encrypted key cache; and

if the mapping exists, then use the mapped symmetric key from the encrypted key cache to decrypt the file, otherwise decrypt the encrypted symmetric key and use the decrypted symmetric key to decrypt the file.

Etzel at col. 7, lines 7-45 is cited as disclosing the elements of claim 1 (see, December 21 Office Action at ¶ 2, p. 2). However, Applicant respectfully submits that there is no discussion in the cited portion of Etzel, or elsewhere in Etzel, of performing a check whether a mapping of the access control entry to the symmetric key exists in an encrypted key cache and if the mapping exists, then use the mapped symmetric key from the encrypted key cache to decrypt the file, otherwise decrypt the encrypted symmetric key and use the decrypted symmetric key to decrypt the file as recited in claim 1. The cited portion of Etzel includes only one reference to a key cache memory, in a sentence that reads "Module 50 stores the CV key in its key cache memory" (see, col. 7, lines 12-13). This sentence is the only mention in the cited portion of Etzel (the paragraph spanning col. 7, lines 7-45) of a key cache memory. Except for stating that a CV key is stored in the key cache memory, there is no discussion or mention of how that key cache memory is used or accessed. Absent such a discussion or mention, and with only a mention that a CV key is stored in a key cache memory, Applicant

respectfully submits that Etzel cannot disclose performing a check whether a mapping of the access control entry to the symmetric key exists in an encrypted key cache and if the mapping exists, then use the mapped symmetric key from the encrypted key cache to decrypt the file, otherwise decrypt the encrypted symmetric key and use the decrypted symmetric key to decrypt the file as recited in claim 1.

Furthermore, as discussed above, the program encryption key of Etzel is used to encrypt a video program, whereas the CV key is used to encrypt the program encryption key. The key cache memory in the cited portion of Etzel stores the CV key, not the program encryption key. The CV key of Etzel is used to exchange in a secure manner encryption keys and other encrypted information (see, col. 5, lines 57-59), not to encrypt a file. As there is no discussion in Etzel of the CV key being used to encrypt a file, Applicant respectfully submits that Etzel cannot disclose a mapped symmetric key from an encrypted key cache as recited in claim 1.

Etzel goes on to discuss key-cache memory locations accessed by security module 215 of a subscriber terminal receiving a message from the video server (see, col. 7, lines 56-66). However, this discussion of key-cache memory locations in Etzel assumes that the encryption key is in the proper key-cache memory location. There is no discussion or mention of checking whether a mapping to the proper encryption key exists, much less of what to do if no such mapping exists. Absent any such discussion or mention, Applicant respectfully submits that Etzel cannot disclose performing a check whether a mapping of the access control entry to the symmetric key exists in an encrypted key cache and if

the mapping exists, then use the mapped symmetric key from the encrypted key cache to decrypt the file, otherwise decrypt the encrypted symmetric key and use the decrypted symmetric key to decrypt the file as recited in claim 1.

For at least these reasons, Applicant respectfully submits that claim 1 is allowable over Etzel.

With respect to claim 5, claim 5 depends from claim 1 and Applicant respectfully submits that claim 5 is likewise allowable over Etzel for at least the reasons discussed above with respect to claim 1. Furthermore, claim 5 recites:

One or more computer-readable media as recited in claim 1, wherein the plurality of instructions further cause the one or more processors to perform the following acts:

generate a file including the encrypted key cache;
encrypt the generated file using a private key of a public/private key pair associated with the user; and
store the encrypted file.

Applicant respectfully submits that Etzel does not disclose to generate a file including an encrypted key cache, to encrypt the file, and to store the file as recited in claim 5. Although Etzel mentions a key cache memory, nowhere is there any discussion or mention to generate a file including that key cache memory, much less to encrypt and store that file. Simply mentioning a key cache memory and storing a key in the key cache memory does not disclose to generate a file including an encrypted key cache, to encrypt the file, and to store the file. As such, Applicant respectfully submits that Etzel does not disclose the elements of claim 5.

For at least these reasons, Applicant respectfully submits that claim 5 is allowable over Etzel.

With respect to claim 6, claim 6 depends from claim 1 and Applicant respectfully submits that claim 6 is likewise allowable over Etzel for at least the reasons discussed above with respect to claim 1. Furthermore, similar to the discussion above regarding claim 5, Applicant respectfully submits that Etzel does not disclose to generate a file including an encrypted key cache and encrypt the generated file as recited in claim 6. For at least these reasons, Applicant respectfully submits that claim 6 is allowable over Etzel.

With respect to claim 7, claim 7 depends from claim 1 and Applicant respectfully submits that claim 7 is likewise allowable over Etzel for at least the reasons discussed above with respect to claim 1. Furthermore, claim 7 recites:

One or more computer-readable media as recited in claim 1, wherein the plurality of instructions further cause the one or more processors to perform the following acts:

obtain, in encrypted form, the encrypted key cache from a remote storage device;

decrypt the key cache using a private key of a public/private key pair associated with the user; and

use, as the encrypted key cache, the decrypted key cache.

Applicant respectfully submits that Etzel does not disclose to obtain an encrypted key cache, in encrypted form, from a remote storage device, to decrypt the key cache and use the key cache as recited in claim 7. Although Etzel mentions a key cache memory, nowhere is there any discussion or mention to obtain the key cache memory, in encrypted form, from a remote source and decrypt and use that key cache memory. Simply mentioning a key cache memory and storing a key in the key cache memory does not disclose to obtain the key cache memory, in encrypted form, from a remote source and decrypt and use that key cache memory. As such,

Applicant respectfully submits that Etzel does not disclose the elements of claim 7.

For at least these reasons, Applicant respectfully submits that claim 7 is allowable over Etzel.

Given that claim 8 depends from claim 7, Applicant respectfully submits that claim 8 is likewise allowable over Etzel for at least the reasons discussed above with respect to claim 7.

Given that claims 2-4 and 9-13 depend from claim 1, Applicant respectfully submits that claims 2-4 and 9-13 are likewise allowable over Etzel for at least the reasons discussed above with respect to claim 1.

With respect to claim 14, Applicant respectfully submits that, similar to the discussion above regarding claim 1, Etzel does not disclose checking whether an access control entry to symmetric key mapping exists in a key cache, and obtaining the symmetric key from the key cache if the mapping exists, otherwise decrypting the encrypted symmetric key using a private key corresponding to the public key as recited in claim 14. For at least these reasons, Applicant respectfully submits that claim 14 is allowable over Etzel.

With respect to claim 18, claim 18 depends from claim 14 and Applicant respectfully submits that claim 18 is likewise allowable over Etzel for at least the reasons discussed above with respect to claim 14. Furthermore, similar to the discussion above regarding claim 5, Applicant respectfully submits that Etzel does not disclose generating a file including the key cache, and encrypting and storing the file as recited in claim 18. For at least these reasons, Applicant respectfully submits that claim 18 is allowable over Etzel.

With respect to claim 19, claim 19 depends from claim 14 and Applicant respectfully submits that claim 19 is likewise allowable over Etzel for at least the reasons discussed above with respect to claim 14. Furthermore, similar to the discussion above regarding claim 6, Applicant respectfully submits that Etzel does not disclose generating a file including the key cache and encrypting the generated file as recited in claim 19. For at least these reasons, Applicant respectfully submits that claim 19 is allowable over Etzel.

With respect to claim 20, claim 20 depends from claim 14 and Applicant respectfully submits that claim 20 is likewise allowable over Etzel for at least the reasons discussed above with respect to claim 14. Furthermore, similar to the discussion above regarding claim 7, Applicant respectfully submits that Etzel does not disclose obtaining a key cache in encrypted form from a remote storage device, and decrypting and using the key cache as recited in claim 20. For at least these reasons, Applicant respectfully submits that claim 20 is allowable over Etzel.

Given that claim 21 depends from claim 20, Applicant respectfully submits that claim 21 is likewise allowable over Etzel for at least the reasons discussed above with respect to claim 20.

Given that claims 15-17 and 22-24 depend from claim 14, Applicant respectfully submits that claims 15-17 and 22-24 are likewise allowable over Etzel for at least the reasons discussed above with respect to claim 14.

With respect to claim 25, claim 25 recites:

A method comprising:
accessing an encrypted key cache, corresponding to a user, in encrypted form;
obtaining an encrypted symmetric key from an access control entry corresponding to the encrypted key cache;

decrypting the encrypted symmetric key using a private key corresponding to the user;

decrypting the encrypted key cache using the decrypted symmetric key; and

using the encrypted key cache to identify, based on access control entries corresponding to other files, symmetric keys used to encrypt the other files.

Applicant respectfully submits that Etzel does not disclose accessing an encrypted key cache, corresponding to a user, in encrypted form, decrypting the encrypted key cache using a decrypted symmetric key, and using the encrypted key cache to identify symmetric keys used to encrypt other files as recited in claim 25.

Etzel at col. 4, lines 9-19 is cited as disclosing the elements of claim 25 (see, December 21 Office Action at ¶ 2, p. 4). However, this cited portion of Etzel discusses decrypting an encrypted program encryption key, and then encrypting a digital video stream using the program encryption key. Nowhere in this cited portion of Etzel, or elsewhere in Etzel, is there any mention or discussion of accessing an encrypted key cache, corresponding to a user, in encrypted form, much less of decrypting the encrypted key cache using a decrypted symmetric key, and using the encrypted key cache to identify symmetric keys used to encrypt other files. Absent such discussion or mention, Applicant respectfully submits that Etzel does not disclose accessing an encrypted key cache, corresponding to a user, in encrypted form, decrypting the encrypted key cache using a decrypted symmetric key, and using the encrypted key cache to identify symmetric keys used to encrypt other files as recited in claim 25.

For at least these reasons, Applicant respectfully submits that claim 25 is allowable over Etzel.

Given that claims 26-28 depend from claim 25, Applicant respectfully submits that claims 26-28 are likewise allowable over Etzel for at least the reasons discussed above with respect to claim 25.

With respect to claim 29, Applicant respectfully submits that, similar to the discussion above regarding claim 1, Etzel does not disclose a comparator to check whether one of the plurality of mappings corresponds to the received access control entry, and a cryptographic engine to use, if one of the plurality of mappings corresponds to the received access control entry, the symmetric key to which the received access control entry maps to decrypt the file, and use, if one of the plurality of mappings does not correspond to the received access control entry, the private key of the public/private key pair to decrypt the symmetric key, and then use the decrypted symmetric key to decrypt the file as recited in claim 29. For at least these reasons, Applicant respectfully submits that claim 29 is allowable over Etzel.

With respect to claim 34, claim 34 depends from claim 29 and Applicant respectfully submits that claim 34 is likewise allowable over Etzel for at least the reasons discussed above with respect to claim 29. Furthermore, similar to the discussion above regarding claim 5, Applicant respectfully submits that Etzel does not disclose to encrypt another file including the key cache, and to store the encrypted file as recited in claim 34. For at least these reasons, Applicant respectfully submits that claim 34 is allowable over Etzel.

With respect to claim 35, claim 35 depends from claim 29 and Applicant respectfully submits that claim 35 is likewise allowable over Etzel for at least the reasons discussed above with respect to claim 29. Furthermore, similar to the

discussion above regarding claim 6, Applicant respectfully submits that Etzel does not disclose to encrypt another file including the key cache as recited in claim 35. For at least these reasons, Applicant respectfully submits that claim 35 is allowable over Etzel.

With respect to claim 36, claim 36 depends from claim 29 and Applicant respectfully submits that claim 36 is likewise allowable over Etzel for at least the reasons discussed above with respect to claim 29. Furthermore, similar to the discussion above regarding claim 7, Applicant respectfully submits that Etzel does not disclose to obtain a key cache in encrypted form from a remote storage device, and decrypt and use the key cache as recited in claim 36. For at least these reasons, Applicant respectfully submits that claim 36 is allowable over Etzel.

Given that claims 32 and 33 depend from claim 29, Applicant respectfully submits that claims 32 and 33 are likewise allowable over Etzel for at least the reasons discussed above with respect to claim 29.

With respect to claim 37, Applicant respectfully submits that, similar to the discussion above regarding claim 25, Etzel does not disclose accessing an encrypted key cache, corresponding to a user, in encrypted form, and decrypting and using the key cache as recited in claim 37. For at least these reasons, Applicant respectfully submits that claim 37 is allowable over Etzel.

Given that claims 38-41 depend from claim 37, Applicant respectfully submits that claims 38-41 are likewise allowable over Etzel for at least the reasons discussed above with respect to claim 37.

With respect to claim 42, claim 42 recites:

A method comprising:

accessing a key cache that maintains a plurality of access control entry to symmetric key mappings corresponding to a plurality of files accessible to a user in a distributed file system, wherein each of the plurality of mappings identifies a symmetric key that can be used to decrypt a file corresponding to the mapping;

generating an encrypted file that includes the key cache and that is encrypted using a symmetric key;

encrypting the symmetric key using a public key corresponding to the user;

storing the encrypted symmetric key in an access control entry corresponding to the encrypted file; and

storing both the encrypted file and the access control entry corresponding to the encrypted file in the distributed file system.

Applicant respectfully submits that Etzel does not disclose generating an encrypted file that includes the key cache and storing the encrypted file as recited in claim 42.

Etzel at col. 3, lines 3-65 and col. 4, lines 9-34 is cited as disclosing the elements of claim 42 (see, December 21 Office Action at ¶ 2, pp. 5-6). However, this cited portion of Etzel discusses generating encryption keys and device unique keys, as well as encrypting a digital video stream using a program encryption key. Nowhere in this cited portion of Etzel is there any mention of a key cache, much less of generating an encrypted file that includes the key cache and storing the encrypted file. Furthermore, there is no mention or discussion anywhere else in Etzel of accessing an encrypted key cache, corresponding to a user, in encrypted form, much less of generating an encrypted file that includes the key cache and storing the encrypted file. Absent such discussion or mention, Applicant respectfully submits that Etzel does not disclose generating an encrypted file that includes the key cache and storing the encrypted file as recited in claim 42.

For at least these reasons, Applicant respectfully submits that claim 42 is allowable over Etzel.

Given that claim 43 depends from claim 42, Applicant respectfully submits that claim 43 is likewise allowable over Etzel for at least the reasons discussed above with respect to claim 42.

With respect to claim 44, Applicant respectfully submits that, similar to the discussion above regarding claim 1, Etzel does not disclose means for comparing the retrieved access control entry to the plurality of access control entry to symmetric key mappings and for determining whether any of the plurality of mappings match the retrieved access control entry, and means for obtaining, from the means for storing, a symmetric key to be used to decrypt the requested file if one of the plurality of mappings matches the retrieved access control entry, and otherwise for decrypting the symmetric key, in encrypted form, using a private key of a public/private key pair corresponding to the public key used to encrypt the symmetric key as recited in claim 44. For at least these reasons, Applicant respectfully submits that claim 44 is allowable over Etzel.

Applicant respectfully requests that the §102 rejections be withdrawn.

35 U.S.C. § 103

Claims 30-31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Etzel in view of U.S. Publication No. 2002/0095590 to Douceur et al. (hereinafter “Douceur”). Applicant respectfully submits that claims 30-31 are not obvious over Etzel in view of Douceur.

The subject application was filed March 26, 2001. Pursuant to 35 U.S.C. §103(c), which was amended effective Nov. 29, 1999 (Public Law 106-113),

Subject matter developed by another person, which qualifies as prior art only under one or more of sub-sections (c), (f), and (g) of section 102 of this title, shall not preclude patentability under this section where the subject matter and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person.

Douceur is cited as prior art under 35 U.S.C. §102(e). Both the subject application and Douceur were owned by, or subject to an obligation of assignment to, the same person or organization at the time the invention of the subject application was made. Given that the filing date of the subject application is after November 29, 1999, Applicant respectfully submits that Douceur is not a useable prior art reference under 35 U.S.C. §103(a) for the above-identified application.

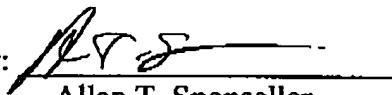
Applicant respectfully requests that the §103 rejections be withdrawn.

Conclusion

Claims 1-44 are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the subject application. Should any matter in this case remain unresolved, the undersigned attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Respectfully Submitted,

Date: 4/20/05

By: 
Allan T. Sponseller
Reg. No. 38,318
(509) 324-9256